A brief history of Internet surveillance policy: and what may happen next…

Caspar Bowden

(Director www.fipr.org 1998-2002)

[these are author's personal views]

CCC Finowurt

13th August 2011

(selective) chronology of privacy regulation

1765: UK Entick vs. Carrington (no "general warrants")

1791: US 4th Amendment (ditto + need probable cause)

1948: UNDHR ("no arbitrary…interference" + right to protection)

1950: ECHR Art.8 (ditto)

1970: 1st DP law in Hesse (Germany)

1973: 1st national DP law in Sweden

1974: US Privacy Act (only public sector)

1978: French DP law

1980: OECD guidelines

1981: Council of Europe Convention 108

1983: German census decision ("information self-determination")

1984: UK DP law

1995: EU Data Protection Directive

2011-: consultations on new EU DP framework

2012-: new US Federal law (DoC green paper, FTC consultation)?

(selective) chronology of covert mass-surveillance

1600s- : Black Chambers, Royal Mail, Mazzini affair
1936-45: ENIGMA, Bletchley, MAGIC, Op-20-G
1945-: GCHQ, NSA, BRUSA, UKUSA
1967: UK "D-Notice" affair
1975: Church Committee
1978: US FISA law, UK "ABC" trial
1985: UK IOCA law ("certificated warrants")
1999: EU report and inquiry into ECHELON
2000: UK RIPA (s.16 authorizes domestic trawling)
2001: 9/11: US PATRIOT, UK ATCSA Pt.11 (data retention)
2003: ~~Total~~ Terrorism Information Awareness furore
2005-: "warrantless wiretapping" exposé
2005: EU Data Retention Directive
2007-: UK "Interception Modernization Program" disclosed, "PROTINT"
2007/8: Protect America 2007, FISA Amendment 2008 (*ex-post* minimisation)
2010: US CALEA 2 rumours
2011: EU DRD revision, US hearings on data retention, cyber-warfare ?

Why worry ?
….and why is this interesting ?

- formulation of constitutional and human rights predated Internet mass-surveillance
- sharp techno-legal dilemmas/dichotomies
  - encryption key escrow vs. reverse burden-proof
  - surveillance by design vs. privacy by design
  - traffic data retention vs. data preservation
- sudden new phenomena
  - social networks, location/mobile platforms,
  - CLOUD COMPUTING
- normal democratic checks-and-balances don't work for <u>covert</u> surveillance policymaking
  - knowledge is power – rule-of-law may be bypassed
  - expedient reliance on private organisations

UK law on Internet surveillance

- Interception of Communications Act 1985 (IOCA)
  - forced by Malone vs. UK 1985 ECtHR
- **Regulation of Investigatory Powers Act (RIPA)** 2000
  - Pt.1.Ch1 – interception of content ("tapping")
  - Pt.1.Ch2. – access to comms data (= traffic + subscriber + location)
  - Pt.3 – decryption powers (dormant until 2007)
  - Pt.4 – "oversight" and complaints
- 9/11 !
- Anti-Terrorism Crime and Security Act 2001
  - Pt.11 – 1st primary legislation on Data Retention in world?
- Wireless Telegraphy Act (lots of revisions since WW1!)
  - authorizes larges scale GSM SIGINT within UK from aircraft?
  - ECHR compliant ?

RIPA 2000 Pt.1 – Interception warrants

- S.5 - “domestic warrant” – targeted at individual
  - one warrant – many copies for ISPs/telcos - maintain “black-boxes” tapping whole stream
  - purposes: serious crime, “safeguarding economic and nat.sec”
  - authorization: signed by Secretary of State (political minister)
  - for communications starting/ending inside UK (??)
  - intelligence/security + police, military, customs agencies
- S.8(4) - “certificated warrant” (trawling) – targeted at search “factors”
  - might utilize ISPs/telcos “black boxes” or other means (direct access to cables?)
  - for international communications” – beginning/ending outside UK
  - same purposes – but performed by GCHQ
  - “factors” described very generally – combo of traffic analysis + keywords + AI
    - ECHELON was in 1970s !
- “oversight” – Interception Commissioner
  - one retired senior judge + some assistants
  - about 6 agencies for interception, hundreds for comms data
  - never written report with significant criticism since 1985 (secret annex?)
  - ~ 2500 interception warrants, ~ 500,000 comms data
    - no breakdown (or mention!) of trawling warrants or traffic data (vs. subscriber account lookup)
- Investigatory Powers Tribunal (IPT)
  - accept any complaints about infringement of human rights in connection with RIPA
  - Panel of retired judges, senior lawyers – security vetted
  - Kafka-esque secret proceedings, no challenging or exposure of evidence to complainants

RIPA 2000 – domestic mass-surveillance warrants (?)

- Section 16(3) – bizarre triple negative wording
  - appears to authorize a 3rd type of warrant
    - allows GCHQ to "look inwards" at UK domestic communications for 3 months at a time
  - Mysterious doctrine of "overlapping warrants"
    - Invented by first IoCC in 1986 (Irish terrorism)
    - no statutory basis
  - debate in House of Lords 2000
    - S.16(3) not replacement for overlapping ??
    - letter to Opposition saying would be illegal to circumvent need for domestic warrant
    - …but suppose domestic warrant "impractical"
    - plenty of loopholes in interaction of 3+ clauses
    - IoCC is judge-and-jury of (secret) interpretation – no caselaw!
  - Could this law be used for mass-surveillance of social networks (press speculation after UK riots, but….)

U.S. Protect America Act 2007 and FISA Amendment Act 2008

- Scandal of "warrantless wiretapping": 2005-2008
  - AT&T technician discovered much US Internet traffic being tapped, triaged, diverted to National Security Agency
  - FISA 1978 required "minimization" of intrusion on US persons
  - To and fro saga of US Administration officials being kept in dark, refusing to re-authorize "Terrorist Surveillance" programs
- FISA Court had rejected major authorization circa 2005: President of Court withheld facts from other judges (!)
  - substance of argument about how hard NSA had to work to prevent collection of data of "U.S. persons"
  - Protect America Act changed to doctrine of minimize-use-not-collection. FISA Court now "approves" policy of ODNI
- **FISAAA 2008 s.1881 authorizes surveillance of "foreign political associations" of non-US persons, and expressly includes Cloud Computing ("remote computing services")**

Questions

- Would it be lawful under ECHR to provide different privacy protection according to nationality (cf. FISA) ?
- How does EU law handle the boundary between "national security" and (former "3rd pillar") "law enforcement" regarding competences/subsidiarity?
- Does EU Data Protection law prohibit or allow intrusions into confidentiality of (a) communications and (b) personal data, under "national security" apparatus of another country?
  - Hint: Safe Harbor, "model clauses", DPD exemptions ?

What are pseudonymous data?

- A pseudonym is an identifier of a subject, in our setting of sender and recipient, other than one of the subject's real names
  - Anonymity, Unlinkability, Unobservability, Pseudonymity, and Identity Management – A Hansen and Pfitzmann

- Whereas anonymity and accountability are the extremes with respect to **linkability** to subjects, pseudonymity is the entire field between and including these extremes. Thus, pseudonymity comprises all degrees of linkability to a subject. Ongoing use of the same pseudonym allows the holder to establish or consolidate a reputation.
  - PRIME space (Dresden Course)

- a transaction is pseudonymous in relation to a particular party if the transaction data contains no direct identifier for that party, and can only be related to them in the event that a very specific piece of additional data is associated with it. The data may, however, be indirectly associated with the person, if particular procedures are followed, e.g. the issuing of a search warrant authorising access to an otherwise closed index
  - Introduction to Dataveillance and Information Privacy, and Definitions of Terms, Roger Clarke, 1997-

EU Data Protection Directive EC 95/46

- Article 2
  - *(a) 'personal data' shall mean any information relating to an identified or identifiable natural person ('data subject'); an **identifiable** person is one who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity;*

The central question: Identifiable by whom?

- Recital 26
  - *Whereas the principles of protection must apply to any information concerning an identified or identifiable person; whereas, to determine whether a person is identifiable, account should be taken of all the **means likely reasonably to be used** either by the controller **or by any other person** to identify the said person; whereas the' principles of protection shall **not apply to data rendered anonymous in such a way that the data subject is no longer identifiable**.*

- Q. "means" – must refer to legal methods as well as statistical methods?
  - Otherwise passport/health-insurance/credit-card numbers would not be personal data (in themselves)
- Q. "means likely reasonably to be used" – must refer to the *method* not the *individual person*?
  - Because otherwise implies a person can be deprived of ECHR Art.8 privacy rights because in a minority!
- Q. "or by any other person" – seems to imply that the following rider "whereas…rendered anonymous" has to be understood as anonymous with respect to "any other person", not merely with respect to the putative data controller?
- Conclusion: if identification might likely reasonably occur by lawful process or statistical means (but even if only happens to a minority of individuals) it **is personal data**.

Key escrow policy UK 1995-1998

- CESG (defensive arm of GCHQ) proposed "Cloud Cover" 1995+
  - peculiar algorithm JMW removes need for "escrow database"
  - Cloud Cover escrowed signature keys (never clear if beyond HMG)!
  - UK shopped around in US – no support
- 1997 (pre-election) consultation on "Licensing of Trusted Third Parties"
  - McGuffin was if want to be licensed TTP, must escrow decryption keys
  - comp.sci term TTP became synonymous with key-escrow
  - unlicensed not prohibited, but no legal umbrella
    - proposed "presumption of validity" for signatures from licensed TTPs
      - at that time, seemed plausible and subtle strategem to coerce escrow adoption
    - (actual UK transposition of e-Sig abandoned entirely – no special status at all)
  - no understanding that self-signed keys for encryption work just fine!
  - summary of consultation "massaged" responses to disguise public hostility to key escrow
  - new UK government reversed ostensible no-escrow policy within 3 months
    - series of civil society meetings: "Scrambling for Safety"
- EU sinks escrow policy by decoupling CSPs from licensing in e-Sig Dir.
  - industry mobilized, policy failing in U.S, finally died in U.K. late '98
  - (FIPR established May 1998)

Power to demand key/passphrase

- Why this is a sharp dilemma
  - Sergienko 1996 says not self-incrimination…
    - Because key no direct "testimonial value" (for RIPA case see here)
  - "Mute of Malice" – better analogy?
- "key escrow" – huge issue in Internet civil society '94-98
  - PGP and hounding of Phil Zimmermann
- RIP 2000 UK civil society campaign
  - 1000 news articles, 15 broadsheet editorials
  - …briefed 100 journalists in 6 months
  - unusually well-informed debate in House of Lords
  - crucial amendment nullifying lost in HoL by one vote!
  - …mainstream TV and Radio wouldn't touch (mostly)
- Lots of material at www.fipr.org/rip/
  - But many dead links ☹

How does RIPA Pt.3 work ?

- Section 49 Notice -
  - for prevention/detection of any crime etc.
  - from same authority as "underlying" power to access data (search warrant/interception warrant etc.)
  - may demand plaintext or key-to-ciphertext
  - may include secrecy order (indefinite ?)
  - may be prosecuted for failure to comply
    - 2 years
    - 5 years for terrorism (2006)/child protection (2007)
- Are terrorists using encryption ?
  - Yes (reports suggest – amateurish "tradecraft")
- Is RIPA Pt.3 causing miscarriages of justice ?
  - Likely (schizophrenic + "55 character" passphrase)

crypto for lawyers - digression

- symmetric key – like a password on a spreadsheet – how send to receiver?
- asymmetric crypto aka "public key" (invented by GCHQ 1973?, before US 1977)
  - means a published key can encrypt (but not decrypt), a (different) "private" key decrypts
  - "solves" (ha!) key distribution problem
  - if you think you have understood 1st time, probably you haven't!
- hybrid crypto
  - session key: choose symmetric key at random
  - encrypt message with session key, encrypt session key with PK
  - best of both worlds – speed of symmetric, power of PK
- digital signature
  - PK operations are "commutative" – i.e. D(E(x)) = E(D(x)) = x
  - what if try other way: encrypt with "private key", decrypt with "public key" (weird!)
  - sort of proves sender must know private key – like a seal (not a signature!)
  - PKI - "public key infrastructure"
  - using digital signatures to create a hierarchy of keys "certified" by "authorities"
  - X.509 – designed for hierarchical (mostly military) organizations (doesn't have to be that way – viz. PGP)
  - PKI – **doesn't** mean a "public infrastructure for keys"
- Steganography (Trimethius *"de re Steganographia",* WW2 crates of watches*)*
  - encrypted data "looks" random => random data can hide encrypted data
  - any data that is compressible contains "arbitrariness" (redundancy) that can be used to hide encrypted data
  - "the steganographer will always get through" – if enough cover traffic
  - any original analog content that has been digitized (but hard to do properly – *anti-stego*)

RIP Bill amended in House of Lords

- 1st concession: must prove once had key
- 2nd concession: no corporate criminal liability
  - stops “key escrow by intimidation”
- 3rd concession – “session key will suffice”
- …final concession: reversing the reversal?
  - if “adduce sufficient evidence to raise the issue”, burdens flips back onto prosecution to prove defendant lying, beyond reasonable doubt
  - what will suffice?
    - no idea 2000-2011.
    - case of Oliver Drage (2010)

Anatomy of VAMP-ware
(Virus Ate My Password)

- Moriarty wants to frame Alice
  - Infect A's machine with memory-resident code
  - Malware
    - Waits until A using machine
    - uses buffer-stuffing or standard API to change key/password
    - Phones home to M when successful
    - Deletes itself from memory
  - Moriarty arranges tip-off to law-enforcement
  - A arrested, machine seized, key demanded
  - No forensic traces of malware on A's machine
    - Traces that key was changed – but A was using at the time
  - S.49 notice is served
  - Plead VAMP at trial
  - What "evidence" can Alice adduce?
- M can use to blackmail A?

Questions

- Is there any satisfactory previous analogy for the situation of using unbreakable digital encryption?
- how might the police show, beyond reasonable doubt, that a defendant is lying about not knowing a key ?....
- is the power to demand a key, with a reversal of the burden of proof, compliant with ECHR?

2001 ATCSA Pt.11 – Data Retention

- UK's PATRIOT Act ("christmas tree")
  - provided for "voluntary" retention by ISPs/telcos
  - reserve power to compel if no co-operation
  - no publication of private govt./industry co-operation agreements
  - same definitions as RIPA Pt.2 (access to data)
    - RIPA fight restricted defn. traffic to exclude browsed URLs!
- Unprecedentedly long argument between Lords and Commons (ping-pong)
  - Amendment won (!) to limit purposes to those "directly or indirectly" related to terrorism
  - wording bungled inexplicably (Bismarck/sausages)
    - not strong enough to have legal effect
- UK began lobbying for EU-wide retention (ECHR?)

Data Retention Directive 15th March 2006 (EC 06/24)

Recital 3: Articles 5, 6 and 9 of **Directive 2002/58/EC** lay down the rules applicable to the processing by network and service providers of traffic and location data generated by using electronic communications services. Such data **must be erased or made anonymous when no longer needed for the purpose of the transmission** of a communication, except for the data necessary for billing or interconnection payments.

Recital 9: …. Because retention of data has proved to be such a necessary and effective investigative tool for law enforcement in several Member States, and in particular concerning serious matters such as organised crime and terrorism, it is necessary to ensure that retained data are made available to law enforcement authorities for a certain period, subject to the conditions provided for in this Directive. The adoption of an instrument on data retention that complies with the requirements of Article 8 of the ECHR **is therefore a necessary measure**.

Article 5 - Categories of data to be retained

- 1. Member States shall ensure that the following categories of data are retained under this Directive:
- (a) data necessary to trace and **identify** the source of a communication:…
- (2) concerning Internet access, Internet e-mail and Internet telephony:
  - (i) the user ID(s) allocated;
  - (ii) the user ID and telephone number allocated to any communication entering the public telephone network;
  - (iii) the name and address of the subscriber or registered user to whom an **Internet Protocol (IP) address**, user ID or telephone number was allocated at the time of the communication;
- (b) data necessary to **identify** the destination of a communication:…
- (2) concerning Internet e-mail and Internet telephony:
  - (i) the user ID or telephone number of the intended recipient(s) of an Internet telephony call;
  - (ii) the name(s) and address(es) of the subscriber(s) or registered user(s) and user ID of the intended recipient of the communication;
- (c) data necessary to identify the date, time and duration of a communication:…
- (2) concerning Internet access, Internet e-mail and Internet telephony:
  - (i) the date and time of the log-in and log-off of the Internet access service, based on a certain time zone, together with **the IP address, whether dynamic or static**, allocated by the Internet access service provider to a communication, and the user ID of the subscriber or registered user;

=> If the purpose (inter alia) of data retention is to identify users from IP addresses, it would be perverse to regard IP addresses as non-identifiable and hence not personal data !

Romanian DRD decision (2009)
(not on grounds of proportionality)

- *The obligation to retain… as an exception or a derogation from the principle of personal data protection and their confidentiality,* ***empties****, through its nature, length and application domain,* ***the content of this principle****... it is unanimously recognized in the ECHR jurisprudence…that the signatory member states… have assumed* ***obligations to ensure*** *that the rights guaranteed by the Convention are* ***concrete and effective, not theoretical and illusory****…* ***the continuous retention*** *of personal data* ***transforms… the exception… into an absolute rule****. The right appears as being regulated in a negative manner, its positive role losing its prevailing role*
- *…the* ***continuous limitation*** *of the privacy right…* ***makes the essence of the right disappear****… mass users of the public electronic communication services or networks, are* ***permanent subjects to this intrusion*** *into their exercise of their private rights to correspondence and freedom of expression, without the possibility of a free, uncensored manifestation, except for direct communication, thus* ***excluding the main communication means used nowadays****.*
- *…justified* **use***… is* ***not*** *the one that in itself harms in an unacceptable way the exercise of the right to privacy or the freedom of expression,* ***but rather the legal obligation with a continuous character, generally applicable, of data retention****… regardless of whether they have committed penal crimes or not or whether they are the subject of a penal investigation or not, which is likely to* ***overturn the presumption of innocence*** *and to transform a priori all users of electronic communication services or public communication networks into people susceptible of committing terrorism crimes or other serious crimes.*
- *…the* ***continuous*** *character of the obligation to retain the traffic and localization data… is* ***unconstitutional in its entirety****…*

Divergences

US

- no 4th Amendment for traffic data
- "3rd party doctrine" – LEA access to private-sector data without court order
- right to be let alone + "reasonable expectation of privacy"
- vertical privacy laws, no private-sector subject access by *right*
- constitutional rights for US persons
- "warrantless wiretapping" 2001-?
  - FISA Amendment 2008 legitimized *ex-post* filtering out of US persons
  - Catch-22 on civil redress
- irreversible shift to "national surveillance state" ? (Balkin 2008)
- mantra: "control usage not collection"
- data-mining programs reported to Congress, but complexity trumps transparency

Europe

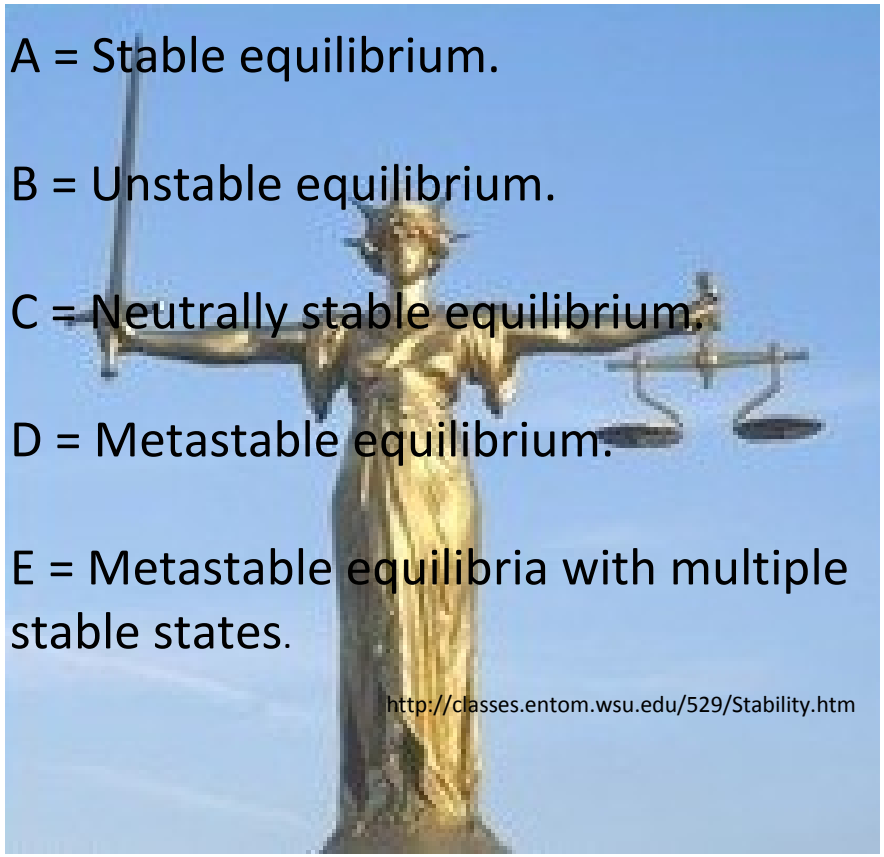
- traffic data protected (Malone v. UK ECHR 1984)
- +ve duty to minimize infringement of broad concept of "private life", privacy as human dignity
- collection of data engages privacy (Rotaru/Amann ECHR), indiscriminate collection deprecated (Marper)
- horizontal Data Protection law, comprehensive subject access right
- human rights independent of nationality
- national security (mostly) exempt from DP law
- Parliamentary and judicial oversight murky at best
- EU/member-state boundary of "national security" clear as mud (ECHELON/Prum/PNR/SWIFT/DRD)

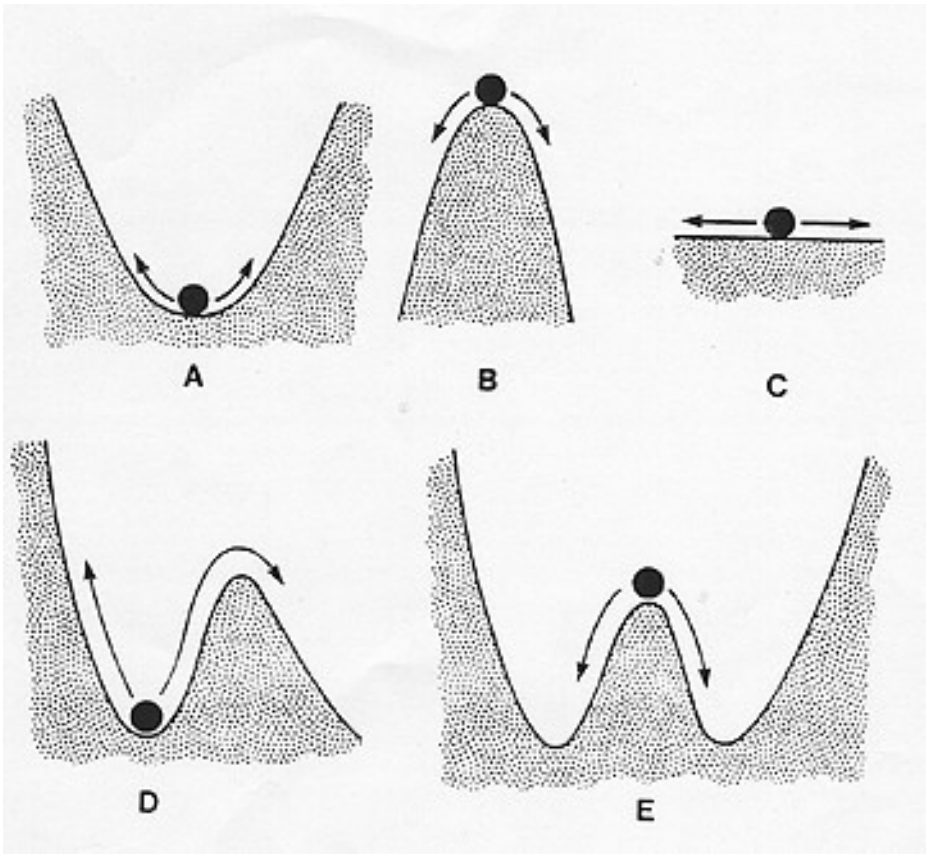
A question of balance ?

…the cliché of first resort…

…how is the balance point decided…

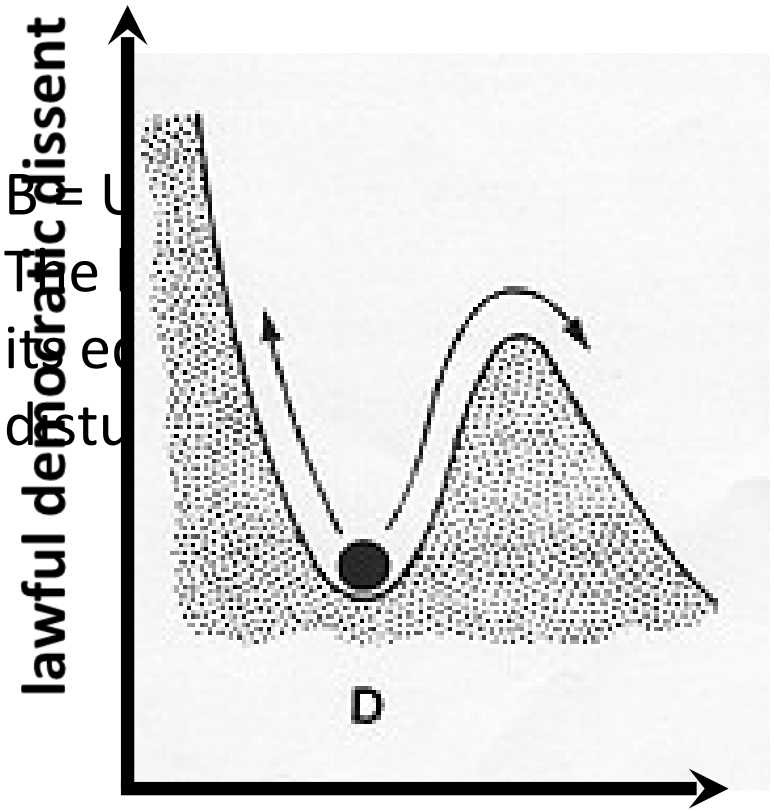
…and what kind of stability?





Slippery slope

…of two kinds…



D = Metastable equilibrium.

if surveillance power increases beyond a critical point, lawful democratic dissent is chilled

intelligentsia will not risk "getting their name on a list"

MORE INSIDIOUS EFFECT THAN "PANOPTIC" CONFORMITY OF OVERT SURVEILLANCE